UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/706,021 | 11/12/2003 | Arnaud Fausse | 09669/009002 | 6206 |

22511 7590 03/05/2010

OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

| EXAMINER | |
|---|---|
| REZA, MOHAMMAD W | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2436 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 03/05/2010 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
buta@oshaliang.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/706,021 | FAUSSE, ARNAUD | |
| | Examiner | Art Unit | |
| | MOHAMMAD W. REZA | 2436 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *17 November 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *7-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *7-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

**DETAILED ACTION**

1. This is in response to the arguments filed on 11/17/2009.

2. Claims 7-20 are pending in the application.

3. Claims 7-20 have been rejected.

## *Continued Examination Under 37 CFR 1.114*

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/17/2009 has been entered.

## *Response to Amendment*

5. The examiner approves the amendments made to claims 7, 8, 10, 11, 13, and 16.

6. The examiner approves addition of new claims 17-20.

7. The examiner approves cancellation of claims 1-6.

## *Response to Arguments*

8. Applicant's arguments with respect to claims 7-20 have been considered but are moot in view of the new ground(s) of rejection.

***Priority***

9. Applicant is reminded that in order for a patent issuing on the instant application to obtain the benefit of priority based on priority papers filed in parent Application of 10/706021 is **a continuation of 09/936645, filed 12/19/2001, 09/936645 is a national stage entry of PCT/FR00/00679, International Filing Date: 03/17/2000 and claims foreign priority to 99/03330, filed 03/17/1999** under 35 U.S.C. 119(a)-(d) or (f), a claim for such foreign priority must be timely made in this application. To satisfy the requirement of 37 CFR 1.55(a)(2) for a certified copy of the foreign application, applicant may simply identify the application containing the certified copy.

***Oath/Declaration***

10. The oath filed on 11/12/2003 complies with all the requirements set forth in MPEP 602 and therefore is accepted.

***Drawings***

11. The drawings filed on 11/12/2003 are accepted.

***Specification***

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

12. The abstract of the disclosure is objected to because it is not in one paragraph,

and it is referred to fig 1. Correction is required. See MPEP § 608.01(b).

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

**Arrangement of the Specification**

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
    (1) Field of the Invention.
    (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).

(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

13. The specification is objected to as failing to provide proper arrangement of the specification. For example, it does not content "BACKGROUND OF THE INVENTION", "BRIEF SUMMARY OF THE INVENTION", "BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING". Necessary correction is required.

14. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

The limitation of claims 7, 10, 13, and 16 are not mentioned in the specification. Particularly: "hash the message" is not mentioned in the specification. Examiner will interpret the particular term as best understood for the basis of the rejection. Necessary correction is required.

***Claim Objections***

15. Claims 7-14 are objected to because of the following informalities:

In claims 7, 10, 13, "inputs/outputs" should be changed to "input/output",

"the link" should be changed to "a link" for the sake of proper antecedent basis,

In claim 8, 10, 11, 13, 14, "the only logic link" should be changed to "a logic link",

"the software" should be changed to "a software",

In claim 9, "display device is a printer, a screen, or a filing device" should be changed to "display device is a printer, or a screen, or a filing device". Appropriate correction is required.

***Terminal Disclaimer***

16. The terminal disclaimer filed on 03/07/2008 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of Patent US 7039808 has been reviewed and is accepted. The terminal disclaimer has been recorded.

***Claim Rejections - 35 USC § 103***

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 7-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holger Sedlak hereafter Sedlak (US Patent 6,510,514) in view of Devaux et al hereafter Devaux (US Patent 6,769,620).

19. As per claim 7, Sedlak discloses an authentication device of a message (**Fig., col. 2, lines 23-26, wherein it states that a device for reliably creating the electronic signature of data includes a data generating device, a data carrier read/write device, and data display device and this data signature is used to verify the integrity of the data)** comprising

a message storage device (**fig., element 1, col. 2, lines 24-25, "a data generating device" which is actually a personal computer (PC) considers as "a message storage device" as well**),

a protected device connected to said message storage device, the protected device configured to ensure protection of the message (**Fig., element 3, col. 2, lines 26-33, "the data carrier read/write device" considers as a "protected device" which is connected to the PC (message storage device). Further, col. 3, lines 25-26 discuss that this device is certified by an approved authority and sealed which means protected and it assures protection of the data that travels from data generating device to the display device**);

a display device connected to said protected device (**fig., element 2, col. 2, lines 31-33, wherein it states that the display device is connected to the data generating device through the data carrier read/write device (protected device)**), wherein the protected device is constituted by a card (**col. 4, lines 6-12, wherein it discloses that read/write device (protected device) has an insertion slot to constitute a smart card**) provided with inputs/outputs I1/01 of commands/data for the link with said message storage device (**Fig., elements 5, and 8, col. 2, lines 43-45, wherein it shows that the data generating device (message storage device i.e. PC) is connected with the data carrier device (protected device) through the read/write link and the connection is input/output basis according to the figure**) and I2/02 of display for the link with said display device (**fig., element 5, col. 2, lines 43-48, wherein it shows that data carrier read/write device (protected device) is**

**connected with the display device through the link. Moreover, col. 4, lines 14-15 states that this connection link could be bidirectional that means it could be input and output both**), physically separate (**it is to be mentioned that Fig. of Sedlak's invention has significant similarity with the fig.1 of the present application by which it shows that the two input/output connections with the data carrier read/write device (Figure, element 3, protected device) with the two specific devices (Figure, element 1 data generating device i.e. message storage device and element 2 display device) are physically separated. Moreover, col. 2, lines 43-45 mention that the protected device is located in between the storage device and display device and thus their connection are physically separated**), wherein the protected device is configured to hash the message received from the message storage device and to send the message to the display device (**col. 2, lines 26-33, wherein it discusses that the data carrier device (protected device) generates the signature of the received data from the data generating device (storage device) and transmits that data to the display device. The signature of the encrypted data is the hash of the data which is discussed in col. 1, lines 16-22. Further, col. 4, lines 7-12 also mentions that the data that receives from the data storage device is encrypted and signed by the protected device**). Although, Sedlak discloses data carrier read/write device (protected device) constitutes with smart card and it is well known that the smart card has the embedded microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is constituted by a microprocessor. However, in the same field of endeavor, Devaux

discloses that the smart card includes the microprocessor (**fig.1, elements 20, and 220, col. 1, lines 4-7, wherein it discusses that the IC card (smart card) has a microcontroller (microprocessor)**).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Sedlak's smart card with a microprocessor as suggest by Devaux. The motivation is that a number of advantages can be obtained; for one, using a microprocessor in the card can run its own program to execute the specific applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

20. As per claim 8, Sedlak discloses the authentication device, characterized in that the only logic link between the commands/data circulating between said protected device and said message storage device on one hand and data circulating between said protected device and said display device on the other hand (**Figure, elements 8, 5, col. 2, lines 27-33, wherein it mentions that the link between data generating device (message storage device) and data carrier read/write device (protected device) in one side and link between display device and data carrier read/write device (protected device) in another side of the protected device and they are based on the data carrying logic),** is the software of said protected device **(col. 4, lines 8-12, wherein it states that algorithm of the smart card to processes the data that transmitted from the data generating device**).

21. As per claim 9, Sedlak discloses the authentication device characterized in that said display device is a printer, a screen, or a filing device **(col. 3, lines 7-8, wherein mentions that the displaying device could be a printer, a screen)**.

22. As per claim 10, Sedlak discloses a card **(col. 4, lines 6-12, wherein it states a smart card)** able to be connected to a message storage device and to a display device **(col. 2, lines 29-33, wherein it states that the card reading device is connected with the data generating device (message storage device) and to a display device)**, characterized in that it is provided with inputs/outputs I1/01 of commands/data for the link with said message storage device **(Fig., elements 5, and 8, col. 2, lines 43-45, wherein it shows that the data generating device (message storage device i.e. PC) is connected with read/write link of the data carrier device (protected device) and the connection is input/output basis according to the figure)** and I2/02 of display for the link with said display device **(fig., element 5, col. 2, lines 46-48, wherein it states that data carrier read/write device (protected device) is connected with the display device through the link. Moreover, col. 4, lines 14-15 states that this connection link could be bidirectional that means it could be input and output both)**, physically separate **(it is to be mentioned that Fig. of Sedlak's invention has significant similarity with the fig:1 of the present application by which it shows that the two input/output connections with the data carrier device (Figure, element 3, protected device) with the two specific devices (Figure, element 1 data generating device i.e. message storage device and element 2 display device) are physically separated. Moreover, col. 2, lines 43-45 mention**

**that the protected device is located in between the storage device and display device and thus their connection are physically separated**), and

characterized in that the only logic link between the commands/data circulating between said card and said message storage device on one hand and data circulating between said card and said display device on the other hand (**Figure, elements 8, 5, col. 2, lines 27-33, wherein it mentions that the link between data generating device (message storage device) and data carrier read/write device (protected device) in one side of the protected device and link between display device and data carrier read/write device (protected device) in another side and they are based on the data carrying logic**), is the software of said card (**col. 4, lines 8-12, wherein it states that algorithm of the smart card to processes the data that transmitted from the data generating device**),

wherein the card is configured to hash the message received from the message storage device and to send the message to the display device (**col. 2, lines 26-33, wherein it discusses that the data carrier device (protected device) generates the signature of the received data from the data generating device (storage device) and transmits that data to the display device. The signature of the encrypted data is the hash of the data which is discussed in col. 1, lines 16-22. Further, col. 4, lines 7-12 also mentions that the data that receives from the data storage device is encrypted and signed by the protected device**).

Although, Sedlak discloses data carrier read/write device (protected device) constitutes with smart card and it is well known that the smart card has the embedded

microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is a microprocessor card. However, in the same field of endeavor, Devaux discloses that the smart card (IC card) is a microprocessor card **(fig.1, elements 20, and 220, col. 1, lines 4-7, wherein it discusses that the IC card has a microcontroller (microprocessor))**.

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Sedlak's smart card with a microprocessor as suggest by Devaux. The motivation is that a number of advantages can be obtained; for one, using a microprocessor in the card can run its own program to execute the specific applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

23. As per claim 11, Sedlak discloses the card, characterized in that the only logic link between the commands/data circulating between said card and said message storage device on one hand and data circulating between said card and said display device on the other hand (**Figure, elements 8, 5, col. 2, lines 27-33, wherein it mentions that the link between data generating device (message storage device) and data carrier read/write device (protected device) in one side and link between display device and data carrier read/write device (protected device) in another side and they are based on the data carrying logic**), is the software of said card (**col.**

**4, lines 8-12, wherein it states that algorithm of the smart card to processes the data that transmitted from the data generating device**).

Although, Sedlak discloses data carrier read/write device (protected device) constitutes with smart card and it is well known that the smart card has the embedded microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is a microprocessor card. However, in the same field of endeavor, Devaux discloses that the smart card (IC card) is a microprocessor card (**fig.1, elements 20, and 220, col. 1, lines 4-7, wherein it discusses that the IC card has a microcontroller (microprocessor)**).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Sedlak's smart card with a microprocessor as suggest by Devaux. The motivation is that a number of advantages can be obtained; for one, using a microprocessor in the card can run its own program to execute the specific applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

24. As per claim 12, Sedlak discloses the card, characterized in that it comprises a physically separate inlet to enter a confidential code (**col. 4, lines 6-12, wherein it describes that the protected device has separate slot to place the card and though the encrypted data transmitted from the data creation device**).

Although, Sedlak discloses data carrier read/write device (protected device) constitutes with smart card and it is well known that the smart card has the embedded microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is a microprocessor card. However, in the same field of endeavor, Devaux discloses that the smart card (IC card) is a microprocessor card (**fig.1, elements 20, and 220, col. 1, lines 4-7, wherein it discusses that the IC card has a microcontroller (microprocessor)**).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Sedlak's smart card with a microprocessor as suggest by Devaux. The motivation is that a number of advantages can be obtained; for one, using a microprocessor in the card can run its own program to execute the specific applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

25. As per claim 13, Sedlak discloses a box able to receive a protected device and able to be connected to a message storage device and to a display device (**col. 2, lines 29-33, wherein it states that the card reading device is connected with the data generating device (message storage device) and to a display device**), characterized in that it comprises a data/command link with said message storage device (**Fig. 1, elements 5, and 8, col. 2, lines 43-45, wherein it shows that the data generating device (message storage device i.e. PC) is connected with read/write**

**link of the data carrier device (protected device**) and the connection is input/output based according to the figure) and the link with said display device (**fig. 1, element 5, col. 2, lines 46-48, wherein it states that data carrier read/write device (protected device) is connected with the display device through the link. Moreover, col. 4, lines 14-15 states that this connection link could be bidirectional that means it could be input and output both**), the inlets/outlets of said data/command link and said display link being electrically independent (**it is to be mentioned that Fig.1 of this reference has significant similarity with the fig:1 of the present application by which it shows that the two links connected with the data carrier device (element 3, protected device) with the two specific devices (element 1 data generating device i.e. message storage device and element 2 display device) are being electrically independent if there is no smart cart in the slot**), and characterized in that the only logic link between the data circulating in the data/commands and display device (**Figure, elements 8, 5, col. 2, lines 27-33, wherein it mentions that the link between data generating device (message storage device) and data carrier read/write device (protected device) in one side and link between display device and data carrier read/write device (protected device) in another side and they are based on the data carrying logic**) is the software of said protected device (**col. 4, lines 8-12, wherein it states that algorithm of the smart card to processes the data that transmitted from the data generating device**),

wherein the protected device is configured to hash the message received from the

message storage device and to send the message to the display device (**col. 2, lines 26-33, wherein it discusses that the data carrier device (protected device) generates the signature of the received data from the data generating device (storage device) and transmits that data to the display device. The signature of the encrypted data is the hash of the data which is discussed in col. 1, lines 16-22. Further, col. 4, lines 7-12 also mentions that the data that receives from the data storage device is encrypted and signed by the protected device**).

Although, Sedlak discloses a data generating device and a display device are connected with the protected device. But he does not expressly mention data/command circuit and a display circuit in the protected device. However, in the same field of endeavor, Devaux discloses that the data/command circuit and a display circuit in the protected device (**fig.1, col. 2, lines 8-15, wherein it shows that the card reader has circuit for data storage and display devices**).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Sedlak's protected device with the circuit for data and display devices as suggest by Devaux. The motivation is that a number of advantages can be obtained; for one, using the circuit for data and display device in the card reader for better control of operation in the reader device (**Devaux col. 2, lines 8-15**). Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

26. As per claim 14, Sedlak discloses the box, characterized in that the only logic link between the data circulating in the data/commands and display device (**Figure, elements 8, 5, col. 2, lines 27-33, wherein it mentions that the link between data generating device (message storage device) and data carrier read/write device (protected device) in one side and link between display device and data carrier read/write device (protected device) in another side and they are based on the data carrying logic**) is the software of said protected device (**col. 4, lines 8-12, wherein it states that algorithm of the smart card to processes the data that transmitted from the data generating device**).

Although, Sedlak discloses a data generating device and a display device are connected with the protected device. But he does not expressly mention data/command circuit and a display circuit in the protected device. However, in the same field of endeavor, Devaux discloses that the data/command circuit and a display circuit in the protected device (**fig.1, col. 2, lines 8-15, wherein it shows that the card reader has circuit for data storage and display devices**).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Sedlak's protected device with the circuit for data and display devices as suggest by Devaux. The motivation is that a number of advantages can be obtained; for one, using the circuit for data and display device in the card reader for better control of operation in the reader device (**Devaux col. 2, lines 8-15**). Known work in one field of endeavor may prompt variations of it for use in either the same field

or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

27. As per claim 15, Sedlak discloses the box characterized in that it is allowing to enter data, such as a confidential code **(col. 2, lines 23-31, wherein it discusses that the read/write carrier device (protected device) is configured to receive secure data)**. But, Sedlak does not disclose the box characterized in that it comprises a keyboard. However in the same field of endeavor, Devaux discloses the box characterized in that it comprises a keyboard **(figure 1, element 12, col. 2, lines 57-60, wherein it shows that the card reader has a keyboard interface to enter the data)**. It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Sedlak's protected device with a keyboard as suggest by Devaux. The motivation is that a number of advantages can be obtained; for one, using the keyboard in the card reader for better control of operation in the reader device and data input flexibility **(Devaux col. 2, lines 57-60)**. Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

28. As per claim 16, Sedlak discloses an authentication device of a message **(Fig., col. 2, lines 23-26, wherein it states that a device for reliably creating the electronic signature of data includes a data generating device, a data carrier read/write device, and data display device and this data signature is used to verify the integrity of the data)**, comprising

a storage device (**fig. 1, element 1, col. 2, lines 24-25, "a data generating device" which is actually a personal computer (PC) considers as a message storage device as well**),

a protected device connected to said storage device, the protected device configured to ensure protection of the message (**Fig:1, element 3, col. 2, lines 26-33, "the data carrier read/write device" considers as a "protected device" which is connected to PC (message storage device. Further, col. 3, lines 25-26 discuss that this device is certified by an approved authority and sealed which means protected) and it assures protection of the data that travels from data generating device to the display device**);

a display device connected to said protected device to form a secure environment (**fig.1, element 2, col. 2, lines 31-33, wherein it states that the display device is connected to the data generating device through the data carrier device (protected device)**),

wherein the protected device comprises a card (**col. 4, lines 6-12, wherein it discloses that read/write device (protected device) has an insertion slot to constitute a smart card**), the card being configured to form a bridge between the storage device and the display device (**(col. 4, lines 6-12, wherein it states that the smart card of the protected device connects the data generating device (message storage device). Further, col. 2, lines 43-46 discusses that the protected device connected in between storage device and display device and bridges between them**),

wherein the protected device is configured to hash the message received from the storage device and to send the message to the display device **(col. 2, lines 26-33, wherein it discusses that the data carrier device (protected device) generates the signature of the received data from the data generating device (storage device) and transmits that data to the display device. The signature of the encrypted data is the hash of the data which is discussed in col. 1, lines 16-22. Further, col. 4, lines 7-12 also mentions that the data that receives from the data storage device is encrypted and signed by the protected device**), and

wherein the storage device is an uncertain zone **(col. 3, lines 60-61, wherein it mentions that the PC is used as a data creation device (storage device) and this data is not certain)** and the display device is a certain zone **(col. 3, lines 3-13, this elaborates that the display device is checking the correctness of the data which considers as a certain zone. But, a PC can not do that which is uncertain region**).

Although, Sedlak discloses data carrier read/write device (protected device) constitutes with smart card and it is well known that the smart card has the embedded microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is constituted by a microprocessor. However, in the same field of endeavor, Devaux discloses that the smart card includes the microprocessor **(fig.1, elements 20, and 220, col. 1, lines 4-7, wherein it discusses that the IC card (smart card) has a microcontroller (microprocessor)**).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Sedlak's smart card with a microprocessor as suggest by

Devaux. The motivation is that a number of advantages can be obtained; for one, using a microprocessor in the card can run its own program to execute the specific applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

29. As per claim 17, Sedlak discloses the authentication device, wherein the display device is configured to display the message received from the protected device, and wherein the message displayed by the display device corresponds to the message hashed by the protected device (**col. 4, lines 22-28, wherein it discloses that the data shown to the display device is coming from the read/write device (protected device) and that data is secured by the protected device. Thus, it ensures that the data shown in the display device and data received from the protected device are identical**).

30. As per claim 18, Sedlak discloses the card, wherein the display device is configured to display the message received from the card, and wherein the message displayed by the display device corresponds to the message hashed by the microprocessor card (**col. 4, lines 22-28, wherein it discloses that the data shown to the display device is coming from the read/write device (protected device) and that data is secured by the protected device. Thus, it ensures that the data shown in the display device and data received from the protected device are identical**).

Although, Sedlak discloses data carrier read/write device (protected device) constitutes with smart card and it is well known that the smart card has the embedded microprocessor (col. 4, lines 6-7). But he does not expressly mention smart card is a microprocessor card. However, in the same field of endeavor, Devaux discloses that the smart card (IC card) is a microprocessor card (**fig.1, elements 20, and 220, col. 1, lines 4-7, wherein it discusses that the IC card has a microcontroller (microprocessor)**).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Sedlak's smart card with a microprocessor as suggest by Devaux. The motivation is that a number of advantages can be obtained; for one, using a microprocessor in the card can run its own program to execute the specific applications (**Devaux col. 1, lines 1-20**). Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces/market place incentives if the variations are predictable to one of ordinary skill in the art.

31. As per claim 19, Sedlak discloses the box, wherein the display device is configured to display the message received from the protected device, and wherein the message displayed by the display device corresponds to the message hashed by the protected device (**col. 4, lines 22-28, wherein it discloses that the data shown to the display device is coming from the read/write device (protected device) and that data is secured by the protected device. Thus, it ensures that the data shown in the display device and data received from the protected device are identical**).

32. As per claim 20, Sedlak discloses the authentication device, wherein the display device is configured to display the message received from the protected device, and wherein the message displayed by the display device corresponds to the message hashed by the protected device **(col. 4, lines 22-28, wherein it discloses that the data shown to the display device is coming from the read/write device (protected device) and that data is secured by the protected device. Thus, it ensures that the data shown in the display device and data received from the protected device are identical**).

## *Conclusion*

33. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOAZZAMI NASSER G can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Mohammad W Reza/

Examiner, Art Unit 2436